Safety Documentation Review

1. Introduction

In support of the Process Control Security Requirements Forum (PCSRF) efforts to establish minimum security criteria for the US industrial control sectors, a review of industrial control safety documents was conducted to determine in what ways, if any, industrial control safety standards affected the PCSRF effort.

The review was conducted with focus on International Standard IEC 61508 – "Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems. IEC 61508 consists of the following parts:

Part 1: General Requirements
Part 2: Requirements for Electrical/Electronic/Programmable Electronic Safety-Related Systems
Part 3: Software Requirements
Part 4: Definition and Abbreviations
Part 5: Examples of Methods for the Determination of Safety Integrity Levels (SILs)
Part 6: Guidelines for the Application of IEC 61508-2 and IEC 61508-3
Part 7: Overview of Techniques and Measures

The review included all parts of IEC 61508 except for Part 4. The review placed emphasis on Parts 1, 2, and 3. The findings are documented in summary form addressing the entire document (General Findings) and with specific discussion of the interesting aspects of the individual parts.

2. General Findings

This standard contains a significant amount of material that has relevance to the security life-cycle and security-assurance case principle for system development. The standard is comprehensive in scope but varies in terms of the detail presented in its various discussion topics. The standard does require some amount of translation and interpretation for proper application in a security context.

The standard does not provide a complete solution that can be applied to solve a particular problem. What the standard offers is a template that can be followed and fleshed out when crafting a specific approach to building safety into a system, taking into account all the aspects that justify the existence of a safety mechanism and then verifying that the mechanism exists in the end product as it was intended to exist.

For the cases were the issues of security and safety overlap, there is strong consistency in the concepts and methods prescribed by the standard in comparison to how they are presented in traditional security material. Where safety and security do not necessarily overlap, the standard provides insight to ways in which security practices can be augmented to leverage the successes of the safety community. The only precaution is that in such cases, the methods must be properly translated into a security context before being applied to solve security problems.

A more detailed discussion of each part of the standard may be found in Section 3, organized by subsection corresponding to the part of the standard (61508-1 in 3.1, 61508-2 in 3.2, etc).

3. Specific Findings

3.1 CEI IEC 61508-1 – General Requirements

General Comments

- This document provides a great reference for organizing and understanding the relationships between the various aspects that make up a program for acquiring, managing and operating a safety critical system. Much of the material has direct correlation to security critical systems. There is some material that requires translation before it can be usefully applied to specific security critical terms.

- It should be noted that the scope of the document is greater than that of the ICS Security Capabilities document.

- The document presents some requirements in a conditional fashion. For example, there may be three conditions (a, b, c) and the system must demonstrate (a) alone or a combination of (b) and (c) to be considered compliant. This is an approach that would serve well in the ICS Security Capabilities document as it evolves into a document that may be employed by the industrial sectors. The use of conditional and selectable criteria makes it possible to establish consensus on the specifics of independent solutions without providing a prescribed design, architecture or integrated solution. The application of conditional and selectable criteria should also be considered because a single document can not possibly account for all instances of systems as they exist in all industrial sectors.

Introduction – p11.

There is good information in this section that places the document, its scope and intended use into context. This section has general material that could be employed to enhance the ICS capabilities document. The areas include:

All relevant lifecycles;
Is not technology specific or technology constraining;
Enables application sector standards to be developed;

Uses safety integrity levels as a means to define the target/objective

This material is useful because it is not specific to any one application; it is sound engineering practices organized into a comprehensive program for employment to acquire safe (or secure) components and systems.

Functional Safety and "Fail-Safe". Another interesting aspect presented by this document is the adoption of a "broad range of principles, techniques and measures to achieve functional safety". This has been done in a manner that excludes the concept of "fail safe". The concept of fail safe was considered inappropriate due to the vast diversity and complexity of contexts in which safety is addressed across application sectors. It was noted that for those cases where failure modes are well-defined and the level of complexity is relatively low, the fail safe concept is appropriate for implementation.

The same line of thinking applies when considering the "broad range of principles, techniques and measures employed to achieve functional security". Functional security only has meaning in the context of the 'function' that is being secured. Halting all operations is a useful fail-secure method – it is sometimes best to not allow any event to occur than to continue to operate with uncertainty in regards to exposures and vulnerabilities. Such an approach will require human intervention to resolve the situation that caused the halt. In critical applications where continuity of operations takes precedence, then this approach may not constitute an optimal solution, and may in fact raise safety issues.

When employing techniques to provide for automated response to security failure conditions, the use of a fail-secure mechanism should be employed when the failure modes are well-defined and the level of complexity is relatively low, just as in the guidance offered for application of Fail-Safe mechanisms.

Section 1.2 g), Safety Life Cycle – p 17. The document uses an overall safety lifecycle model as the technical framework for dealing systematically with the activities necessary for ensuring the functional safety of the system.

An associated note points out that the life cycle aspect makes it possible to develop safety requirements specifications in a systematic, risk-based manner.

This section provides useful commentary that should be incorporated in security documents used as guidance, best practice or of a tutorial nature supporting the use of the ICS Security Capabilities and its derivative documents.

Section 1.2 j), Note that this section does not explicitly state that it excludes security concerns. However, the text states that the standard "… does not cover precautions necessary to prevent unauthorized persons damaging, and/or otherwise adversely affecting the functional safety of the safety-related systems."

It may be concluded that any organization that follows this standard as written will not be implementing security measures to protect their safety systems. It may be appropriate for the industrial sectors to initiate action to begin looking at security of their safety systems.

Section 4, Conformance to the standard. The standard presents the following conceptual discussion:

> The degree to which a requirement is satisfied (degree of rigor) is not able to be defined in the absence of consideration of the specific environment and conditions in which the requirement is implemented. These factors include: nature of the hazard, consequence of risk reduction, safety integrity level, type of implementation technology, size of system, number of teams involved, physical distribution of components, and novelty of design.

The issues presented in this paragraph from the standard should be captured in either the ICS Security Capabilities document or in its associated guidance/application documentation. The text requires some amount of translation and interpretation to capture the security issues where they differ from the safety perspective as presented by the standard.

Section 5.1, 5.2 – Objectives. The two objectives of the standard are to 1) define the information that must be documented to ensure that all phases of the safety lifecycle can be performed, and 2) define the information that must be documented so that the management of the functional safety verification/assessment processes can perform their functions.

It should be noted that the ICS document does not ensure "all" phases of the safety life cycle are performed; the ICS document focuses on the product/system development and integration. Also, I would add that the ICS does one thing that the standard does not: it defines the criteria to be used in developing the security capabilities and in verifying that those capabilities have been properly implemented.

Figure 2, page 33. The depicted Overall Safety LifeCycle is appropriate for adopting in the ICS Security Capabilities document. It should be noted that the standard presents a comprehensive discussion of the life cycle, and some of the parts of the standard serve only to elaborate a single portion of the overall safety life cycle depicted in Part 1 of the standard.

Table 1, beginning page 39. The material captured in the table is relevant to the ICS Security Capabilities from the standpoint of the process and activities that are conducted to generate and use the ICS Security Capabilities document.

3.2 CEI IEC 61508-2 – Requirements for Programmable Safety-Related Systems

General Comments

- This part of the standard focuses on the requirements for hardware design and implementation. As such it discusses concepts of safety integrity levels. The safety integrity levels have a large amount of focus on detecting and recovering from hardware faults and failures. While that is a significant issue for h/w intensive components, it has limited conceptual application to software (because s/w does not fail). On the other hand, there may be faults in the specification, design or implementation of s/w intensive systems and therefore, there is applicability of this section to security should the ability to detect and recover from non-secure states be required.

- Part 2 page 15 provides discussion which places this part of the standard in context. Whereas Part 1 General Requirements outlines the entire safety life cycle, this part focuses on subsystems and components and provides direction to refine the information developed in accordance with Part I for design and manufacture of hardware components. Note that software components are addressed in Part 3 and, the software discussion is not as complete as the hardware discussion. The reason is that the s/w is implemented to run on target h/w, therefore, the combination of h/w and s/w is addressed in this part of the standard and the s/w portion is limited to the s/w development process.

- The design and manufacture requirements include those for installation, commissioning and final validation, and includes these issues as they relate to modification of equipment. This material has direct correlation to the material contained in the ICS capabilities document.

- While this section does not specifically address operation and maintenance activities, it does address preparation of information required for operations and maintenance.

- This Part, as does Part 1, defines a structured approach to building safety into the system; this approach has relevance to achieving similar goals for security.

Section 7 – General

- This section amplifies the portion of Part I that address the realization of the system (i.e., taking it from concept to an operating entity). Safety requirements are defined in terms of safety functional and safety integrity requirements. Note also that safety integrity requirements encompass defined safety integrity levels (SILs). This line of thinking has direct application to the security line of thinking but does require translation and interpretation.

Section 7.4.6 – Requirements for System Behavior on Detection of a Fault

- Despite the focus on hardware, this section presents useful information that can be applied in the context of security related mechanism or component fault detection and recovery should such be a desired capability of the security system.

Section 7.4.8 – Requirements for Data Communications

- There are data communication requirements levied against the safety system should inter-process communication be necessary in providing the safety capabilities. These requirements are what a security engineer would classify as fundamental security issues affecting the integrity and availability of the system. The scope of these requirements are:
  - Transmission error
  - Repetitions
  - Deletion, insertion
  - Re-sequencing
  - Corruption
  - Delay
  - Masquerade

Two important notes:

1) Specific criteria for the behavior of the safety system were not defined, that is left to the requirements specification for the individual system. The importance of this is that it illustrates that while there may be guidance provided by this standard (as is guidance provided by SP99 et al), there remains the need to explicitly define the requirements for the target system (as is being done through varying levels of abstraction by the PCSRF effort).

2) There is clear documented overlap between the principles behind a safe system and the principles behind a secure system. All security and safety documents must be reviewed to ensure that where the overlap is dealt with, there is consistency and cohesiveness.

Section 7.5 Integration

- An impact analysis is required should any component of the safety system be modified as a result of integration testing. The impact analysis identifies all components affected by the change and the re-verification activities required after the change is implemented.

  This exact concept is fundamental to what I refer to as “continuity of assurance”, where the security established at one point in time must be documented and maintained as the system, over time, evolves.

Section 7.7 Safety Validation

- This refers to establishing confidence that all components meet their safety functional and safety integrity requirements. The material in this section is a good candidate for incorporation into any security-related document (perhaps with some translation or interpretation).

Section 7.8 Modification

- This refers to establishing confidence that safety integrity is maintained after corrections, enhancements or adaptations to the safety systems. The material in this section is a good candidate for incorporation into any security-related document (perhaps with some translation or interpretation).

Section 7.9 Verification

- This refers to establishing confidence that the output of a given phase of the safety life cycle is consistent with and correct in regards to the inputs to that phase of the safety life-cycle. The material in this section is a good candidate for incorporation into any security-related document (perhaps with some translation or interpretation).

- A very important concept of this section is that of entry and exit criteria. Entry and exit criteria establish the threshold that must be crossed when moving from/to adjacent pairs of the life cycle process.

3.3 CEI IEC 61508-3 – Software Requirements

Section 1 – Scope

- Safety-related s/w includes all the following:
    - Operating Systems
    - System s/w
    - Communication s/w
    - Human-computer interface s/w
    - Support tool s/w (Development, design, language translators, testing, debugging, configuration management)
    - Application program s/w

  The scope includes firmware as used in any of the above instances. While such a classification helps to translate the scope into meaningful terms, the safety related s/w is that software which direct provides or indirectly enables the safety functions of the system. The same is true for security software.

Section 6 – Software Quality Management System

- 6.2.2 A strategy is required for the procurement, development, integration, verification, validation and modification of safety s/w. The strategy is targeted at meeting the requirements mandated by the SIL allocated to the s/w.

  This concept has direct relevance to developing and employing a strategy for security. The key is the assurance level allocated to the s/w. This is the essence of what PCSRF is trying to do beyond defining the functional capabilities of the security components.

- 6.2.3 S/w configuration management requires a life-cycle approach to configuration management. It is noted in the standard that management decision and authority is required to guide and enforce the use of configuration management controls.

  Another note refers to ISO/IEC 12207 for information on configuration management.

  It should be noted that for security the same buy-in from management is required (decision and authority). It would be useful to review ISO/IEC 12207 for relevance and perhaps use in SP99 and other related efforts to the PCSRF effort.

Section 7 – Software Safety Lifecycle Requirements

- The emphasis is on ensuring that each phase of the s/w safety lifecycle provides meaningful information to the other phases. Flexibility is allowed in that an organization may choose not fully explicitly follow the structure and form of ISO 61508; a s/w lifecycle process/methodology may be substituted so long as the objectives and requirements of this standard are met.

- 7.3.2 Relevant modes must be defined, such as:
  - preparation for use to include setting and adjustment
  - startup; teach; manual; semi-automatic, automatic; steady state operation
  - Resetting; shut-down; maintenance
  - Reasonably foreseeable abnormal conditions

This is excellent guidance and it illustrates that the s/w engineering process is a dynamic process and if it is to be applied effectively there must be flexibility to do what is best for the given situation.

3.4 CEI IEC 61508-4 – Definitions and Abbreviations

This section was not reviewed.

3.5 CEI IEC 61508-5 – Examples of Methods for the Determination of Safety Integrity Levels

This document provides discussion to aid in understanding the elements of risk and associates the risk concepts to safety, safety integrity levels and assurance.

The term ALARP (as low as reasonably practical) is introduced and used. The fundamental concept is that for each instance of an identified safety issue, risk must be quantified and the ALARP concept applied such that one of the following three determinations may be made:

1. the risk is so great that it must be refused altogether,
2. the risk is or has been made so small as to be insignificant,
3. the risk falls between the two conditions stated in 1 and 2. This implies that the risk exists, is not insignificant but through prudent measures, has been reduced as far as is reasonably practical. This represents “tolerable risk”.

The remainder of the document provides a detailed overview of the process, tying together the concepts of safety requirements definition and allocation, risk identification, and definition of safety integrity levels (quantitatively, qualitatively).

The material in this section has conceptual application to security and may be applied conceptually to develop equivalent information and arguments to support a security case (where the security case is a statement of claims about the “goodness” of the security capabilities in relation to vulnerability and risk, a body of evidence and arguments to support the claims).

3.6 CEI IEC 61508-6 – Guidelines for the Application of IEC 61508-2 and IEC 61508-3

This document is very detailed and technical in meeting the objective of illustrating how to employ Parts 2 and 3 of the standard. Annex A, although informative, provides a good series of steps to follow in implementing the safety program with focus on the requirements determination, design, implementation and testing aspects of the safety life-cycle.

It should be noted that the standard has defined Section 2 to be all the requirements to be satisfied by the safety process with focus on hardware, and Section 3 is only the software part. Therefore, section 2 must always be included when utilizing Section 3. Another important point is that many hardware components include firmware, and firmware typically follows the s/w development process prior to being loaded into hardware.

This document has aspects that are extremely technical with discussion of h/w failure probability determination, h/w reliability estimation, etc., and advanced s/w techniques such as communicating sequential processes (CSP) and formal method proofs of correctness.

3.7 CEI IEC 61508-7 – Overview of Technical Measures

This document provides a comprehensive reference to the technical measures that may be employed to implement aspects of a safety program. The measures are categorized into 4 annexes that address the following hardware and software issues: A – Control of Random H/W Failures; B – Avoidance of Systematic Failures; C – Overview of Techniques and Measures for Achieving Software Safety Integrity; D – A Probabilistic Approach to Determining Software Safety Integrity for Pre-Developed S/W.

References to published material are provided and the measures are presented in a terse overview fashion. The reader will need to consult the references if not familiar with the details of the technical measure or it proper application.

The material in this document is most appropriate for the engineer that is prescribing the methods employed singularly or in combination to verify correctness of the safety system implementation.

The material in this document does not provide criteria to aid in selection of the best method for a specific situation or to meet a specific objective.